



DIVISION OF LAW ENFORCEMENT
11181 SUN CENTER DRIVE
RANCHO CORDOVA, CA. 95670
Telephone: (916) 464-1200
Fax: (916) 464-5577

November 16, 2009

Darren Tsang
Criminal Justice Specialist
California Emergency Management Agency
3650 Schriever Avenue
Mather, CA 95655

Re: First Quarter Progress Report - HT09019504

Dear Mr. Tsang:

During the first quarter (July – September 2009), the Advanced Training Center (ATC) presented one PC Forensics – Data Collection (Basic Data Recovery and Acquisition – BDRA) course. This course was presented in Santa Barbara from September 21 - 24, 2009. Out of the 24 students attending, 12 were from a High Technology Task Force. This course continues to be an important starting point for officers responsible for seizing and imaging digital evidence. The students gained knowledge they will utilize in future classes, as well as in laboratory and field operations. The course received excellent reviews from the students and they look forward to future forensic courses.

The ATC also worked on updating their class material to ensure the students are aware of the latest methods used by criminals committing high technology crimes. The students are trained on the latest criminal trends involving electronic equipment, such as cellular phone and Global Positioning System (GPS). These types of devices are commonly used by criminals who commit sex offenses involving children, identity theft, murder, and drug-related crimes.

In addition to updating class material for existing courses, the ATC developed a new block of instruction on emerging GPS technologies and trends. This entailed purchasing, researching, and beta-testing a wide spectrum of devices. First, research was conducted on GPS technology; the varied GPS coordinates; and how they are interpreted, converted and transferred between devices. A PowerPoint presentation was created to acquaint the students with the basic understanding of the earth and its coordinates and most importantly, the concept of how coordinates are recorded and applied to a position on earth.

Next, baseline images were created of each GPS device to demonstrate in class how different devices vary from each other when tracking changes occur and data is stored. Furthermore, file structure and details of each individual device were noted and will be explained in the PC Forensics – Investigations Advanced course. These devices will then be used in similar and dissimilar areas to demonstrate the varied data storage methods.

The next step was to research, test and use each of the forensic tools that can be utilized to examine each device. Arrangements were made between the ATC and software companies to beta-test their tools in exchange for free license(s). These tools are then used on each individual device to compare their results.

A proper amount of information, demonstration and hands-on examinations were considered in the development of a course that would sufficiently allow students to effectively examine and report on the analysis of a GPS device.

California law enforcement agencies continue to be overwhelmed with the number of criminal cases involving cell phones. Many times the cell phones will be seized by law enforcement officers and checked for evidence connecting the suspect to the crime. However, being able to view the phone's contents may be challenging because the phone may have an activated PIN (password protected). The Cellular Phone Forensics/Investigation class, scheduled to be presented in January 2010, will now include an expanded discussion that will teach the officers how to obtain a PIN from PIN locked phones.

iPhones continue to gain popularity, and many vendors of cell phone forensic software/hardware have added increased abilities for iPhones. The ATC has been successful in arranging for some of these companies to loan their software/hardware for the students to use during class. In return, these companies are able to introduce their products to law enforcement agencies. Cell phones' Subscriber Identity Module or SIM cards contains personal identity information, cell phone numbers, contact information, text messages and other data. An expanded block detailing cell phones' capabilities will be added to the upcoming Cellular Phone Forensics/Investigation course.

In preparation for the second quarter, the ATC has begun purchasing the equipment that is required for the students to build their own forensic computer in the PC Forensics – Investigations Advanced course; forensic cell phone kits issued to students in the Cellular Phone Forensics/Investigations course and; Macbook laptops have been ordered to present the newly developed LINUX in Computer Forensics/Macintosh course. Both the PC Forensics - Specialized Investigative Tools class, and the first of two PC Forensics – Investigations Advanced courses will be presented during the second quarter reporting period.

The ATC continues to receive positive feedback and success stories from students who have attended the High Technology Computer Crimes series of classes in the past. Listed below are a few testimonials that were recently submitted to the ATC from students who attended the PC Forensics – Investigations Advanced course in June 2009. The students credit the ATC in providing the needed training and equipment used to investigate these cases.

Case: I

A suspect molested his seven-year-old step-daughter at their family-owned business while the girl's mother was attending night school. The victim said that when her mother was gone, the suspect closed the business doors and showed the victim sex videos from an adult pornography website. The suspect then took the victim to a bed in the back office and asked her to reenact the sex scenes. According to the report, this happened at least five times; often enough for the victim to remember the website's exact name. The victim was too young to know any specific dates, but she knew it had occurred within the past year. This was based on the date the business was opened and the dates when the mother attended night school.

As taught in PC Forensics – Investigations Advanced course, Internet Explorer leaves evidence in six places (daily history, weekly history, visited history, Typed URLs, cache files, cookie files) on a computer. In this case, the laptop was configured to delete Internet history and cache automatically. This left very little "active" evidence to examine. Therefore, the officer had to dig for bits and pieces of these various logs from unallocated and deleted spaces. The officer also examined several dozen of Windows XP "Restore Points" for archived Registry files with Typed URLs.

The officer then assembled all the fragmented pieces from eight source types into a timeline of when pornography sites were accessed (an hour one day, a few hours another day, etc.). Those timelines were then compared to the known times when the suspect was babysitting the victim and while the mother was in school. Of course, no match can positively confirm that she was molested on any given day. This is because there were other dates, when the suspect may have visited the specified pornography site by himself. However, the fact that the only pornography site found on the computer was the exact site mentioned by the seven-year-old victim. This was very compelling evidence that corroborated victim's statements. Furthermore, the computer forensics evidence was the only physical evidence in this entire case.

Case: II

This is a case where a suspect killed his wife's young lover. The suspect's computer had very little evidence, but had Map Quest driving directions from his city to the residential intersection where the victim was killed. In addition, there were also web queries regarding the victim's employer. All hits were found only in Google Desktop files.

The investigating officer used the software issued to him in the PC Forensics – Investigations Advanced class to make a virtual machine. He then installed a new Google Desktop program and copied the suspect's Google Desktop database files to the virtual machine.

The officer was then able to search the computer's web history by date. The officer was able to prove that the suspect conducted the relevant web searches a few weeks prior to the murder. The officer could also prove that the suspect first misspelled the business name before he finally spelled it correctly. This also enabled the officer to view the actual caches of the web files that are usually encrypted or compressed. Those files also showed that the suspect had logged into his yahoo email at the same time as the computer searches. The suspect was arrested and charged with murder.

Case III:

An officer recently testified at a jury trial of a man who was being charged with multiple crimes including possession of bombs; silencers and; home-made zip guns with the intent of killing his ex-wife, her attorney, the police investigator and the family court judge. This defendant was also found in possession of a stolen handgun and the identification of a deputy sheriff.

The subsequent forensic analysis of the suspect's computer revealed that the suspect had conducted Internet background searches on all of the victims. He had also conducted surveillance of the victims' homes. The suspect took pictures of the victims, their homes and their vehicles. The suspect also used the stolen sheriff's identification card to counterfeit a new identification card bearing his own information in order to further his crimes. The forensic analysis also revealed letters and emails from the suspect in which he professed his dedication and intention to kill the victims.

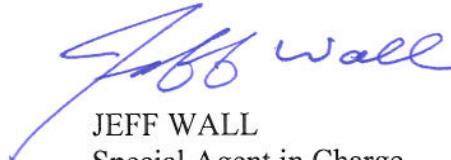
The crux of this case was the evidence found on the computer. The jury found the defendant guilty of the charges and he was later sentenced to 18 years in prison.

The investigating officer believes that a major disaster and loss of life was prevented by his investigation including the forensic computer examination. He learned those valuable skills in the PC Forensics – Investigations Advanced course, presented by the ATC.

All scheduled classes for the 2009/2010 Fiscal Year are presently full. A one-year-long student waiting list continues to grow longer. The popularity of these courses is a testament to their necessity.

The continued funding and support from the California Emergency Management Agency will ensure the continued availability of these crucial computer forensic courses. By funding these courses, the CalEMA is improving the effectiveness of California's law enforcement officers. It is clear that the aforementioned computer forensic courses provide crucial training that enables law enforcement officers to identify dangerous criminals. As a result of their investigative efforts, the investigating officers are able to and provide prosecutors with the evidence that is necessary to ensure effective prosecutions. In conclusion, it is through the computer forensic courses that are offered by the ATC, that a greater level of public protection is achieved.

Sincerely,

A handwritten signature in blue ink that reads "Jeff Wall". The signature is stylized, with the first name "Jeff" written in a cursive script and the last name "Wall" in a more straightforward, slightly cursive font.

JEFF WALL
Special Agent in Charge

For EDMUND G. BROWN JR.
Attorney General